REMARKS

Claims 1-36 are pending in the present application. Claims 1, 3-5, 7-11, 13, 15-17, 19-23, 25, 27-29, and 31-35 were amended. Reconsideration of the claims is respectfully requested.

Amendments were made to the specification to correct errors and to clarify the specification. No new matter has been added by any of the amendments to the specification.

I. 35 U.S.C. § 112, Second Paragraph

The examiner has rejected claims 1-36 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter, which applicants regard as the invention.

Claim 1 was rejected for failing to clearly indicate the purpose of the method claimed. The preamble of claim 1 has been amended to specify that the method is directed to managing a composite keystore generated from local keystores of users. Withdrawal of the rejection to claim 1 under 35 U.S.C. § 112, second paragraph, is respectfully requested.

Claim 2 was rejected due to the dependency on claim 1. Claim 1 has been amended, and thus the rejection of claim 2 is now moot.

Claim 3 was rejected for failing to clearly indicate how the "determining" step relates to the other steps of claim 1. Claim 3 has been amended to clearly indicate that the "determining" step is performed in response to determining that the one or more certificates do not preexist in the preselected portion of the distributed database. Additionally, the claim term "invalid" was asserted as being vague and indefinite. Applicants note the term invalid is explicitly defined in the subject application (See Page 12, Lines 21-22), and is thus neither vague or indefinite. Withdrawal of the rejection to claim 3 under 35 U.S.C. § 112, second paragraph, is respectfully requested.

Claim 4 was rejected as being dependent on rejected claim 3. Claim 3 has been amended to overcome the rejections under 35 U.S.C., second paragraph, and thus the rejection of claim 4 is now moot.

Claim 5 was rejected for failing to clearly indicate the goal for the new certificate is requested and from where the new certificate is requested. Claim 5 has been amended to clarify that the new certificate is requested by the composite keystore and that the new certificate is a valid certificate that corresponds to the invalid certificate. Withdrawal of the rejection to claim 5 under 35 U.S.C. § 112, second paragraph, is respectfully requested.

Claim 6 was rejected under 35 U.S.C. 112, second paragraph, for being indefinite. Particularly, claim 6 has been rejected as "incomplete since the step of updating recited in" claim 6 does not cooperate with any other steps recited earlier in the parent claim. As described in the subject application, an update event may result from various scenarios, e.g., a user update, an automatic update, and may be performed independent of the method steps of claim 1. Therefore, the rejection of clam 6 is in error, and withdrawal of the rejection of claim 6 under U.S.C. 112, second paragraph, is requested.

Claim 7 was rejected for failing to specify from where the new certificate is requested. Claim 7 has been amended to specify that the new certificate is requested by the composite store, and withdrawal of the rejection of claim 7 under 35 U.S.C. 112, second paragraph, is thus requested.

Claim 8 was rejected as incomplete since the steps of determining and replacing are not recited as cooperating with any other steps in parent claim 1. Claim 8 has been amended to clarify that the claim 8 step of determining is performed responsive to the claim 1 step of determining that any of the one or more certificates preexists. Additionally, the claim limitation of "replacing said preexisting certificate with said current certificate" has been amended to clarify that it is performed "responsive to determining the current certificate supercedes the preexisting certificate." Withdrawal of the rejection of claim 8 under 35 U.S.C. § 112, second paragraph is thus requested.

Claim 9 was rejected for lack of an antecedent basis of the claim term "distributed keystore." Claim 9 has been amended to recite a "distributed database" rather than a "distributed keystore" and thus has proper antecedent basis. Additionally, claim 9 was rejected for failing to set forth the ultimate goal for which a selected certificate is requested. Claim 9 has been amended to clearly recite that the selected certificate is used for encrypting data to be transferred in secured data transfer. Additionally, claim 9 was rejected as being incomplete for failing to set forth cooperation of the claim 9 steps. Claim 9 has been amended to clearly set forth that the claim 9 step of "requesting a selected certificate" is performed responsive to the claim 9 step of "accessing said distributed database." Additionally, claim 9 was rejected for failing to further limit the method of parent claim 1. However, the claim 9 steps of "accessing said distributed database" and "requesting a selected certificate" are performed independent of, and in addition to, the claim 1 method steps (See Figure 5, steps 502 and 504 and corresponding description). As the claim 9 method steps are performed in addition to the claim 1 method steps, claim 9 clearly further limits claim 1. Accordingly, withdrawal of the rejections to claim 9 under 35 U.S.C. § 112, second paragraph has been overcome, and such a notice is respectfully requested.

Claim 10 was rejected for failing to set forth the ultimate goal of the searching step of claim 10. Applicants respectfully disagree. Claim 10 recites that the step of "searching the local database for said selected certificate" is performed "in response to a failure of" the parent claim 9 step "of requesting a selected certificate." Applicants submit that the goal of searching for the selected certificate in a local keystore when a previous request for the selected certificate from the composite keystore has failed is evident in view of the detailed description – that is to obtain a certificate that was not obtained by a request for "said selected certificate" from the composite keystore. Additionally, the "selected certificate" searched in the local database as recited in claim 10 is described as being used for encrypting data to be transferred in claim 9. Accordingly, withdrawal of the rejection to claim 10 under 35 U.S.C. § 112, second paragraph has been overcome, and such a notice is respectfully requested.

Claims 11 and 12 were rejected for depending from claim 8 that was rejected for indefiniteness. Claim 8 has been amended hereinabove to overcome the rejections thereto, and thus the rejections to claims 11 and 12 are now moot.

Additionally, claims 13-24 and 25-36 were rejected in parallel with claims 1-12 as having similar problems of indefiniteness. Claims 13-24 and 25-36 have been amended in similarly manner to claims 1-12. Applicants submit that each of clam 13-24 and 25-35 are sufficiently amended to overcome the 35 U.S.C. 112, second paragraph, rejections thereto, and thus withdrawal of the rejections of claims 13-36 under 35 U.S.C. 112, second paragraph is requested.

Therefore the rejection of claims 1-36 under 35 U.S.C. § 112, second paragraph has been overcome.

II. <u>35 U.S.C. § 103, Obviousness</u>

The examiner has rejected claims 1, 2, 6, 7, 11, 13, 14, 18, 19, 23, 25, 26, 30, 31 and 35 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,049,872 to Reiter et al (hereinafter Reiter) in view of U.S. Patent No. 6,418,467 to Schweitzer et al. (hereinafter Schweitzer). This rejection is respectfully traversed.

With respect to the rejection of claim 1, the Office Action states the following:

> Reiter et al (6,049,872) teaches (see for example, Brief Summary Text - BSTX (4); Detailed Description Text - DETX (14), (2); and Claim Text - CLTX (36)]:
>
> (1) a method comprising the steps of
> (a) retrieving/reading
> (i) information/file/data/code/certificate
> (1) from a source storage [i.e., a PGP (or POP) key server that is local to a region in the world]; and
> (b) storing/writing/saving
> (i) the retrieved information/certificate
> (ii) into a destination storage [i.e., a database (of PGP certificates) that is maintained by a Path Server].
>
> However, Reiter does not teach:
> (1) determining/checking
> (a) where if
> (i) the information/certificate retrieved from a source storage
> 1) pre-exist in a destination storage
> (b) prior to storing the information/certificate into a destination storage.
>
> Schweitzer et al (6,418,467) teaches [Abstract; Detailed Description Text - DETX(71)]
> (1) prior to updating a database,
> (a) identifying discarding duplications
> (i) thereby enhancing the efficiency of data repository.
>
> It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:
>
> (1) apply the teaching of Schweitzer so as to identify and avoid duplications of information/certificates that are being stored into Reiter's destination storage/database.

> The skilled person would have been motivated to do this application because:
>
> (1) Schweitzer teaches that the application of avoiding of the duplications enhances the efficiency of updating a database by gathering information from a plurality of source database; and
>
> (2) Reiter's teaching is related to the field of updating database by merging information from a plurality of sources into a consolidated database.
>
> Office Action dated 08/06/2004, page 5.

Applicants respectfully disagree. To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

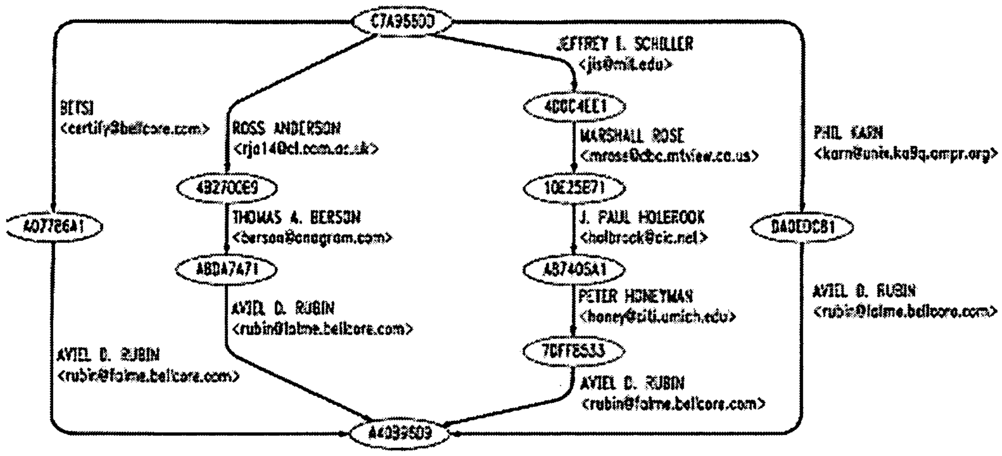
The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

In this particular case, no teaching or suggestion of all the claim limitations is provided in the cited references. Additionally, there is no suggestion or motivation, either in Reiter or Schweitzer or in the knowledge generally available to one of ordinary skill in the art, to combine the reference teachings. Moreover, no reasonable expectation of success for reaching the presently claimed invention by combining the teachings of Reiter and Schweitzer exists. For example, amended claim 1 recites the following:

> 1. A method of managing a composite keystore generated from user local keystores comprising the steps of:
>
> retrieving one or more certificates from a local database of a user, wherein the certificates are associated with the user;
>
> responsive to retrieving said one or more certificates, determining if any of said one or more certificates preexists in a preselected portion of a distributed database of the composite keystore; and
>
> storing nonpreexisting certificates of said one or more certificates in said preselected portion of said distributed database.

The system described by Reiter provides a mechanism for a process of authenticating channels in a distributed system for communications involving a path of channels. For example, Figure 1 of Reiter is as follows:

FIG. 1



As can be seen, Reiter uses multiple paths in an authentication process for authenticating a channel by providing a graphical representation of paths from a trusted key (C7A966DD) to a query key (A40B96D9) to be authenticated. The graph is built from a database of PGP certificates obtained *from various key servers*. The user is then able to verify the paths exists.

The passages[1] of Reiter cited in the rejection of claims 1, 2, and 11 are as follows:

> The authentication process in centralized computer systems is simplified by the fact that there is a central authority (the operating system, or a security kernel thereof) that controls all channels and knows which principals can initiate requests on which channels. In a distributed system, however, typically no such central authority exists for this information. As the distributed system gets larger and more diverse, the difficulty of reliably authenticating a channel increases substantially. An in a system as large and diverse as the Internet, reliably authenticating a channel presents a heretofore impossibly complicated task. Reiter, Column 1, Lines 19-30
>
> PathServer provides a World Wide Web interface by which a user can submit a path length bound, PGP identifiers for a source key (e.g., her own) and a target key, and a choice of disjoint or connective paths, and will receive in real time a display of the requested paths. An example is shown in FIG. 1, which is the result of specifying disjoint paths of length at most eight with a source key identifier of C7A966DD and a target key identifier of A40B96D9. The service generates this information using a graph built from a database of PGP certificates, which PathServer updates periodically *from other PGP key servers* throughout the

world.; (*emphasis added*)
Reiter, Column 6, Lines 1-12

PathServer maintains a database of PGP certificates that is updated periodically *from several other POP key servers* throughout the world. (*emphasis added*).
Reiter, Column 6, Lines 57-59

b) a database being coupled to the processor and storing a plurality of PGP certificates, wherein said database includes an interface for receiving periodic updates *from a plurality of PGP key servers;* (*emphasis added*).
Reiter, Column 17, Lines 23-27

Thus, Reiter explicitly states that the PGP database is built and updated from "key servers." Reiter provides no description or suggestion for retrieving one or more certificates "from a local database of a user."

As described in the subject application, certificates are retrieved from local keystores for users in a system to form a composite keystore. For example, Figure 3 of the subject application shows the following:

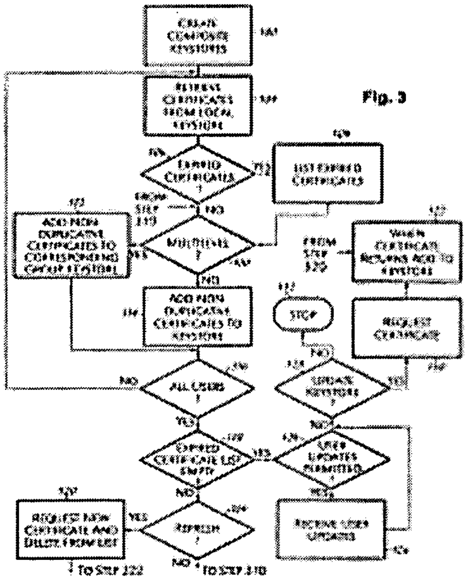


Fig. 3

As can be seen, certificates are retrieved from local keystores of a user (step 304), and an evaluation is made determine if additional users are available in the system for retrieving their local keystores (step 316). Processing returns to step 304 to retrieve the local keystores of any additional users until all users keystores have been retrieved. A composite keystore is thus aggregated by retrieving user keystores on a user-by-user basis (See Page 12, Lines 15-18; Page 14, Lines 15-17).

In addition to failing to describe or suggest a method for retrieving one or more certificates "from a local database of a user," Reiter additionally fails to describe or suggest a method of determining if the one or more certificates retrieved from a local database of a user preexists in a preselected portion of a distributed database of the composite keystore, as the Examiner concedes. However, the Examiner asserts that Schweitzer describes a method for determining if one or more certificates retrieved from a local database of a user preexist in a preselected portion of a distributed database. Applicants respectfully disagree.

Schweitzer describes a system for capturing network traffic information that is collected by gatherer devices. The information collected by the gatherer devices is correlated with account information to facilitate transaction accounting. Manager devices store the gathered information in a central database so that usage based billing may be performed. For example, Figure 1 of Schweitzer shows the following:

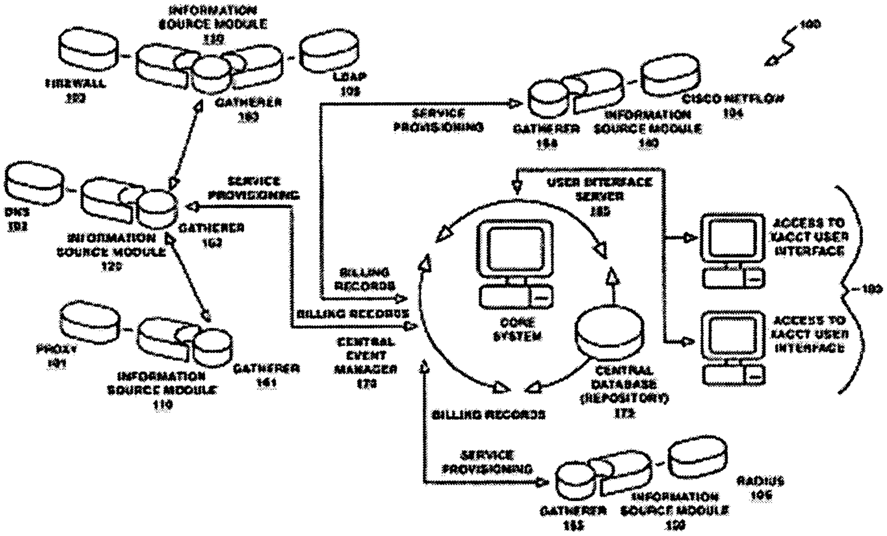

INFORMATION SOURCE MODULE 130
FIREWALL 103
GATHERER 163
LDAP 105
SERVICE PROVISIONING
GATHERER 164
INFORMATION SOURCE MODULE 140
CISCO NETFLOW 104
100
DNS 102
SERVICE PROVISIONING
GATHERER 162
INFORMATION SOURCE MODULE 120
USER INTERFACE SERVER 185
ACCESS TO XACCT USER INTERFACE
ACCESS TO XACCT USER INTERFACE
180
BILLING RECORDS
BILLING RECORDS
CORE SYSTEM
PROXY 101
INFORMATION SOURCE MODULE 110
GATHERER 161
CENTRAL EVENT MANAGER 170
CENTRAL DATABASE (REPOSITORY) 175
BILLING RECORDS
SERVICE PROVISIONING
GATHERER 165
INFORMATION SOURCE MODULE 150
RADIUS 106

FIG. 1

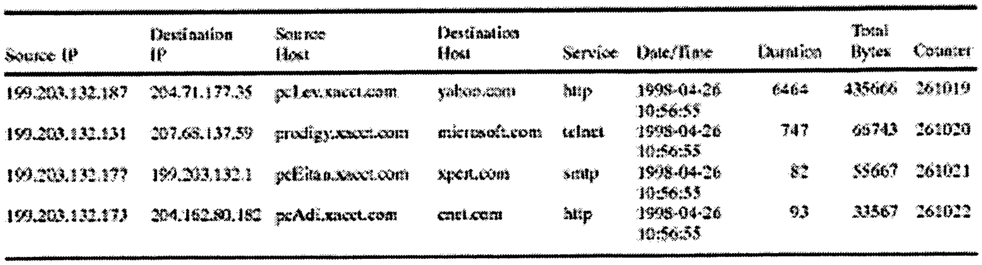
As can be seen, a central database (175) is used for a central repository of information collected in the system (100) by various gatherers (161-165) that interface with information source models (ISMs 110, 120, 130, 140, and 150). The ISMs collect the data that is retrieved by the gathers to be placed in the central database.

In rejecting claim 1, the Office Action cites the following passage[2] of Schweitzer as teaching the method of determining if the one or more certificates retrieved from a local database of a user "preexists in a preselected portion of a distributed database":

> As each IP session may generate multiple *transaction records*, during the merge process the CEM 170 identifies and discards duplications, enhancing the efficiency of the data repository. Generally, *data records* are passed through the merger program, in the CEM 170, into the central database 175. However, the *data records* are also cached so that if matching records appear at some point, the already stored records can be replaced or enhanced with the new records. The database tables that contain the record flows can be indexed, enhancing the efficiency of the data repository. A merge is achieved by matching some of the fields in a *data record* and then merging the matching records from at least two record flows, transforming them into one record before updating the central database 175. In some embodiments, adaptive tolerance is used to match records. Adaptive tolerance allows for a variation in the values of fields that are compared (e.g., the time field value may be allowed to differ by some amount, but still be considered a match). The adaptive aspect of the matching can include learning the appropriate period to allow for the tolerance. The reason that the records that do not match any previous records are sent through into the central database 175, in addition to being cached for later matching, is to avoid loss of data in case of system failure. (*emphasis added*).

Schweitzer, Column 9, Lines 23-46.

Thus, Schweitzer only describes mechanisms for recording "transaction records" or "data records" in a database, mechanisms for identifying duplications, and replacing and enhancing records. Schweitzer in no manner describes or suggests a methodology for determining if any of "one or more certificates" retrieved from "a local database of a user" preexist in a preselected portion of a distributed database. For example, Schweitzer shows the following table containing types of records stored in the central database (175):



Source IP	Destination IP	Source Host	Destination Host	Service	Date/Time	Duration	Total Bytes	Counter
199.203.132.187	204.71.177.35	pcLev.xacct.com	yahoo.com	http	1998-04-26 10:56:55	6464	435666	261019
199.203.132.131	207.68.137.59	prodigy.xacct.com	microsoft.com	telnet	1998-04-26 10:56:55	747	65743	261020
199.203.132.177	199.203.132.1	pcEitan.xacct.com	xpert.com	smtp	1998-04-26 10:56:55	82	55667	261021
199.203.132.173	204.162.80.182	pcAdi.xacct.com	cnet.com	http	1998-04-26 10:56:55	93	33567	261022

Reiter, Column 9, Lines 49-63.

As can be seen, the database stores session information data, such as source and destination IP addresses, source and destination hosts, the service provided, dates, times, duration, and data quantities involved in the session. That is, the database stores "information on network sessions" (Column 9, Lines 9-10). Moreover, Schweitzer recites the following with regard to the ISMs that provide the interface for the gatherers from which the manager devices accumulate the information in the central database:

> The following ISMs are available in some embodiments of the invention.
>
> Categorizer--Classifies a session to a category according to user-defined Boolean expression.
>
> DNS (e.g. ISM 120)--Resolves host names and IP addresses.
>
> Generic Proxy Server (e.g., ISM 110)--Collects data from access logs in a
>
> common log format.
>
> Port/Protocol Resolution--Converts protocol/port information to account names and vice versa.
>
> CheckPoint FireWall-1--Collects data from FireWall-1 accounting log and security log.
>
> Cisco IOS IP Accounting--Collects accounting data from a Cisco router using IOS IP accounting.
>
> Cisco NetFlow Switching--Collects session data from a Cisco router via NetFlow switching.
>
> Netscape Proxy Server--Collects data from a Netscape Proxy Server.
>
> Microsoft Proxy Server--Collects data from a Microsoft Proxy Server.

Schweitzer, Column 5, Lines 52 - Column 6, Lines 6.

Schweitzer in no manner describes, suggests, or otherwise alludes to determining if any of one or more "certificates retrieved from a local database of a user" preexist "in a preselected portion of a distributed database." In fact, Schweitzer makes no mention of user certificates as Schweitzer is wholly unrelated to trusted party authentication mechanisms and thus has no usage for, in general, performing any operation on user certificates and, in particular, for determining if user certificates exist in a distributed database.

Independent claims 13 and 25 recite similar features as claim 1 and were rejected with the same rational applied to claim 1. Therefore, the same distinctions between Reiter and Schweitzer and the claimed invention in claim 1 apply for these claims. As discussed above, Reiter fails to describe or suggest a method of retrieving one or more certificates "from a local database of a user" and for determining if one or more certificates retrieved from a local database of a user "preexists in a preselected portion of a distributed database." Additionally, Schweitzer fails to describe or suggest a methodology for determining if any of "one or more certificates" retrieved from "a local database of a user" preexists in a preselected portion of a distributed database, and in fact Schweitzer is wholly unrelated to user certificates and trusted party authentication mechanisms. Thus, Schweitzer is thoroughly insufficient to provide for the deficiencies of Reiter. For these reasons, Reiter and Schweitzer do not contain all elements of independent claims 1, 13, and 25, and thus the teachings of the references fail to render the claims *prima facie* obvious. Hence, Reiter and Schweitzer fail to obviate the present invention as recited in claims 1, 13, and 25. Since claims 2, 6, 7, and 11 depend from claim 1, claims 14, 18, 19, and 23 depend from claim 13, and claims 26, 30, 31, and 35 depend from claim 25, the same distinctions between Reiter and Schweitzer and the claimed invention in independent claims 1, 13, and 25 apply for these claims. Additionally, claims 2, 6, 7, 11, 14, 18, 19, 23, 26, 30, 31, and 35 claim other additional combinations of features not suggested by Reiter and Schweitzer. Consequently, it is respectfully urged that the rejection of claims 1, 2, 6, 7, 11, 13, 14, 18, 19, 23, 25, 26, 30, 31, and 35 under 35 U.S.C. § 103(a) as being unpatentable over Reiter in view of Schweitzer have been overcome, and such a notice is respectfully requested.

Moreover, no suggestion or motivation exists, either in Reiter or Schweitzer or in the knowledge generally available to one of ordinary skill in the art, to modify the references or to combine reference teachings, nor would a reasonable expectation of success exist. As discussed above, Reiter is directed to a mechanism for a process of authenticating channels in a distributed system for communications involving a path of channels, while Schweitzer is directed to methods for capturing network traffic information that is collected by gatherer devices to facilitate usage billing in a network, Schweitzer is wholly unrelated to trusted party authentication mechanisms and thus has no use for performing any operations or database storage of user certificates as a user certificate, e.g., key and signature data, would serve no function in facilitating gathering of network traffic information. Likewise, the teachings of Schweitzer for gathering network usage information would server no function toward facilitating channel authentication mechanisms described by Reiter. Thus, thus the teachings of the references are not sufficient to render the claims *prima facie* obvious as no motivation for combining the reference teachings exists.

Additionally, the examiner has rejected claims 3-5, 15-17, and 27-29 under 35 U.S.C. § 103(a) as being unpatentable over Reiter in view of Schweitzer and further in view of U.S. Patent No. 6,529,953 to Van Renesse (hereinafter Van Renesse). This rejection is respectfully traversed.

Van Renesse generally describes a system for monitoring and locating computer network resources. One or more hierarchical management information bases (HMIBs) is deployed that allows users to locate and obtain information regarding network resources. The system includes a plurality of nodes and each node maintains a portion of the HMIB. The user starts from the local node and navigates through the system using contact information that is part of the HMIB. A root management information base (MIB) contains information regarding every participating node and a user can obtain the contact information in the root MIB maintained by the node for more detailed information about any participating node. For example, Figures 2A and 2B of Van Renesse show the following:

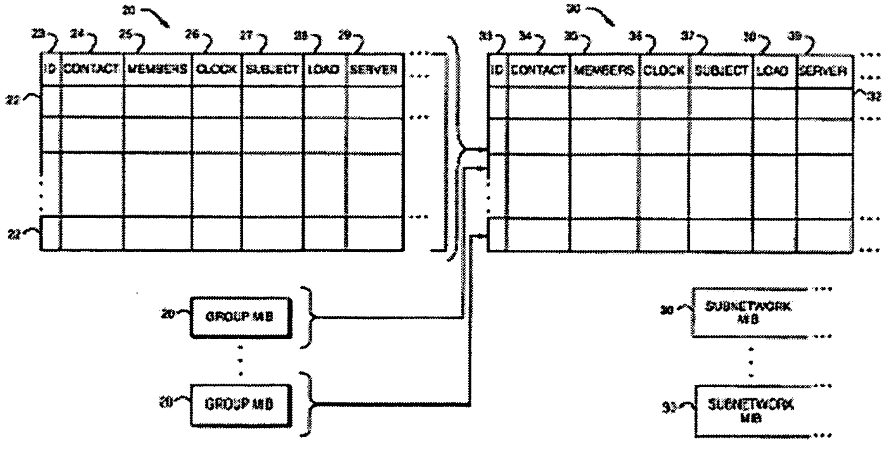


FIG. 2A

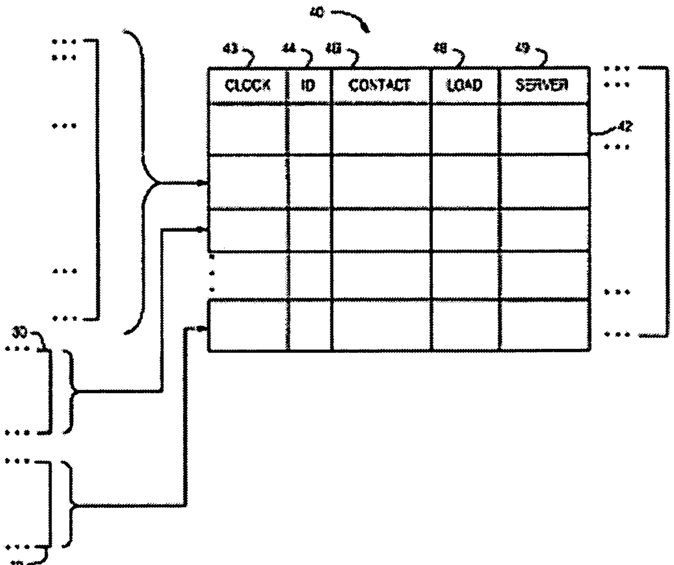


FIG. 2B

As can be seen, nodes supply information, such as load, contact, and the like, to an MIB (20). Each row contains an identifier (23) that specifies the node is the source of the information in the corresponding row. To accommodate additional hierarchical levels, information in the MIB is condensed to become a row (32) of a subnetwork MIB (30). For the next higher level, the subnetwork MIB is condensed as row (42) of a network MIB (40).

With regard to the rejection of claim 3, the Examiner states the following:

> In case if a certificate is checked to see whether it is correctly signed an a certification authority:
>
> (1) Van Renesse (6,529,953) teaches [see Detailed Description Text - DETX (28), (29)]
>
> (a) determining,
>
> (i) prior to updating a certificate,
>
> (ii) if
>
> (iii) a certificate is invalid/"correctly signed".
>
> In case if a certificate is checked to see whether it is in error:
>
> (1) It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:
>
> (a) check the information being read out from a storage, (whether the read information being a certificate or any other type of information), for error before further handling that read information; and
>
> (b) to realized that in a reliable memory reading apparatus, an error detection is provided for detecting the invalidity of the information being read out.

(2) The skilled person would have been motivated to:

(a) check retrieved information for error because:

(i) it is a common practice in the art to make sure that read information:

(1)can be corrected if the read information has error and

(2) if has errors and cannot be corrected, then ignore it (or else it will be used and result in an error);

(ii) it is a common practice in the art of memory/storage/database error detection to include an error detection to detect error in the information being read from a memory/storage/database.

Office Action dated 08/06/2004, Page 8.

Applicants respectfully disagree. Claim 3, as amended, recites the following:

> 3. The method of claim 1 further comprising, responsive to determining that said one or more certificates do not preexist in the preselected portion of the distributed database, determining if said one or more certificates is invalid.

The passage[3] of Van Renesse cited by the examiner as teaching the method of "determining if said one or more certificates is invalid" in response to determining that the "one or more certificates do not preexist in the preselected portion of the distributed database recites the following:

> Each MIB is assigned a public/private key pair. The private key is given to all nodes that store the MIB, and the nodes use the key to sign the updates of the MIB. The update message then contains an associated authentication certificate that includes the MIB identifier and the corresponding public key, and is signed by a certification authority with a well-known public key.
>
> When a node receives an update for a particular MIB, the node checks that the included certificate is correctly signed by the certification authority and that the update is correctly signed in accordance with the public key contained in the certificate. If the update is valid, the node uses the information contained therein to update the appropriate entries in the MIB. This mechanism ensures that only those nodes that maintain that MIB can update the MIB, since only those nodes have the private key required to sign the updates.

Van Renesse, Column 7, Lines 39-54.

The passage of Van Renesse recites only conventional public key/private key encryption mechanisms. Particularly, when a node receives an update to an MIB, the node checks that a certificate included with the update is correctly signed by the certification authority and that the update is correctly signed in accordance with the public key contained in the certificate. This ensures that only nodes allowed to make an update to an MIB are restricted to nodes having the appropriate private key required to sign the update. Van Renesse does not describe or suggest determining if a certificate is invalid "responsive to determining that said one or more certificates do not preexist in the preselected portion of the distributed database," but rather only evaluates a certificate to determine if a node should be able to modify an MIB. Van Renesse provides no description or suggestion for building a composite keystore database, and thus clearly fails to evaluate a certificate in response to determining the certificate does not preexist in a database. Thus, Van Renesse is insufficient to provide for the deficiencies of Reiter and Schweitzer.

Claims 15 and 27 recite similar features as claim 3 and were rejected with the same rational applied to claim 3. Therefore, the same distinctions between Reiter, Schweitzer, and Van Renesse and the claimed invention in claim 3 apply for these claims. For these reasons, Reiter, Schweitzer, and Van Renesse do not contain all elements of claims 3, 15, and 27, and thus the teachings of the references fail to render the claims *prima facie* obvious. Since claims 4-5 depend from claim 3, claims 16-17 depend from claim 15, and claims 28-29 depend from claim 27, the same distinctions between Reiter, Schweitzer, and Van Renesse and the claimed invention in claims 3, 15, and 27 apply for these claims. Additionally, claims 4-5, 16-17, and 28-29 claim other additional combinations of features not suggested by Reiter, Schweitzer, and Van Renesse. Consequently, it is respectfully urged that the rejection of claims 3-5, 15-17, and 27-29 under 35 U.S.C. § 103(a) as being unpatentable over Reiter in view of Schweitzer and further in view of Van Renesse have been overcome, and such a notice is respectfully requested.

Moreover, if an independent claim is non-obvious under 35 U.S.C. 103, then any claim depending therefrom is non-obvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Thus, claims 3-5, 15-17, and 27-29 are non-obvious as Applicants have already demonstrated claims 1, 13, and 25 to be in condition for allowance. Applicants respectfully submit that claims 3-5, 15-17, and 27-29 are also allowable, at least by virtue of their dependence on an allowable base claim.

Additionally, the examiner has rejected claims 8, 12, 20, 24, 32, and 36 under 35 U.S.C. § 103(a) as being unpatentable over Reiter in view of Schweitzer and further in view of U.S. Patent No. 5,212,788 to Lomet et al. (hereinafter Lomet) or U.S. Patent No. 6,584,475 to Carey et al. (hereinafter Carey). This rejection is respectfully traversed.

Lomet describes a distributed database having a plurality of databases at different nodes. A mechanism for timestamping data in the distributed database includes two phases. In the first phase, each cohort votes to commit or abort the transaction and also provides a vote of an earliest and latest time at which the transaction is to be committed. If all cohorts vote to commit the transaction and the intersection of the vote times is nonempty, then the transaction is committed at a time selected from the intersection in the second phase.

With regard to claim 8, the Office Action recites the following passage[4] of Lomet:

> Furthermore, each datum or record 120 in the distributed database is timestamped, which means that along with the datum or record is stored a consistent set of time values indicative of the order in which the values in those records were last updated. In addition, to the current values of the records stored in the database, the database preferably also stores old versions of records 122 which have since been updated. By storing data which has been superceded by updated values, the database enables one to determine the status of the database at any specified time in the past.

Lomet, Column 3, Lines 10-20.

Thus, Lomet describes a mechanism for storing timestamp values in records that indicate the order in which record values were updated. Lomet, however, is wholly unrelated to trusted party authentication mechanisms and thus provides no description or suggest for performing any operation on user certificates. Lomet in no manner describes, suggests, or otherwise alludes to a methodology of determining if a current certificate supercedes a preexisting certificate in response to determining any of one or more certificates preexists, nor for replacing a preexisting certificate with a current certificate if the current certificate supercedes the preexisting certificate. Thus, Lomet is thoroughly inadequate to provide the deficiencies of Reiter and Schweitzer described above.

Carey describes a system for controlling database growth in a read-repeatable environment. An erase list is maintained in each generation of a database and is used to control growth of the database. The erase list is used to identify obsolete pages which can be removed from the database.

With regard to claim 8, the Office Action recites the following passage[5] of Carey:

> Each generation includes one or more pages (or records) which provide the various values of the database table columns. A page is a unit of allocation, typically 4 k bytes or 8 k bytes, by which the information within the database is made available to a user. As updates are made to the database, these pages are superceded by subsequent versions of the page which reflect the changes made by the most recent update. In some instances, a difference between a new generation and its immediate predecessor may be a single change in one of these pages--the remaining records which make up the two generations remaining identical.

Carey, Column 1, Lines 22-32.

Thus, Carey describes pages that are superceded by subsequent versions of the pages. However, Carey is utterly silent with regard to trusted party authentication mechanisms and thus provides no description or suggest for performing any operation on user certificates. Particularly, Carey in no manner describes or suggests a methodology for determining if a current certificate supercedes a preexisting certificate in response to determining any of one or more certificates preexists, nor for replacing a preexisting certificate with a current certificate if the current certificate supercedes the preexisting certificate. Thus, Carey is thoroughly inadequate to provide the deficiencies of Reiter and Schweitzer described above.

Claims 20 and 32 recite similar features as claim 8 and were rejected with the same rational applied to claim 8. Therefore, the same distinctions between Reiter, Schweitzer, and Lomet and Carey and the claimed invention in claim 8 apply for these claims. Since claim 12 depends from claim 8, claim 24 depends from claim 20, and claim 36 depends from claim 32, the same distinctions between Reiter, Schweitzer, Lomet and Carey and the claimed invention in claims 8, 20, and 32 apply for these claims.

Moreover, if an independent claim is non-obvious under 35 U.S.C. 103, then any claim depending therefrom is non-obvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Thus, claims 8, 12, 20, 24, 32, and 36 are non-obvious as Applicants have already demonstrated claims 1, 13, and 25 to be in condition for allowance. Applicants respectfully submit that claims 8, 12, 20, 24, 32, and 36 are also allowable, at least by virtue of their dependence on an allowable base claim.

Accordingly, withdrawal of the rejection of claims 8, 12, 20, 24, 32, and 36 under 35 U.S.C. § 103(a) as being unpatentable over Reiter in view of Schweitzer and further in view of Lomet or Carey is respectfully requested.

Additionally, the Examiner has rejected claims 9, 10, 21, 22, 33, and 34 under 35 U.S.C. § 103(a) as being unpatentable over Reiter in view of Schweitzer and further in view of U.S. Patent No. 5,899,998 to McGauley et al. (hereinafter McGauley). This rejection is respectfully traversed.

McGauley describes a distributed database for storing medical information. The system is self-updating and uses point-of-service stations at locations where patients may carry a portable data carrier that contains medical histories of the patents. Interaction between the portable data carriers and the point-of-service stations effect a virtual link that ties the databases together without online or live data connections. The point-of-service stations also interconnect over a communications network. The database system uses an update object to distribute data that has been generated when a portable data carrier is not physically present and automatically distributes data without the necessity of accessing a masterfile.

With regard to claim 9, the Office Action cites the following passage[6] of McGauley as teaching the method of accessing the distributed keystore and requesting a selected certificate from the distributed keystore:

> Although the presently preferred distributed database architecture is relatively fail-safe on its own because it distributes the data independently throughout the system and does not rely on a central station or masterfile, the administrative services system's database can be used to backup the distributed PDC and POS databases when necessary.

McGauley, Column 14, Lines 56-61.

Thus, McGauley describes a distributed database architecture that does not rely on a central station, and in no manner describes, suggests, or otherwise alludes to accessing a keystore nor for requesting a selected certificate. The passage recited of McGauley only makes a general reference to a distributed database architecture. In fact, McGauley is wholly unrelated to trusted party authentication mechanisms and thus provides no description or suggest for performing any operation on a distributed keystore or user certificates. Thus, McGauley is thoroughly inadequate to provide the deficiencies of Reiter and Schweitzer described above.

Claims 21 and 33 recite similar features as claim 9 and were rejected with the same rational applied to claim 9. Therefore, the same distinctions between Reiter, Schweitzer, and McGauley and the claimed invention in claim 9 apply for these claims. Since claim 10 depends from claim 9, claim 22 depends from claim 21, and claim 34 depends from claim 33, the same distinctions between Reiter, Schweitzer, and McGauley and the claimed invention in claims 9, 21, and 33 apply for these claims.

As discussed above, McGauley fails to describe or suggest a method of "accessing a distributed keystore" and for "requesting a selected certificate from said distributed keystore" and thus is insufficient to provide for the deficiencies of Reiter and Schweitzer. For these reasons, Reiter, Schweitzer, and McGauley do not contain all elements of claims 9, 10, 21, 22, 33, and 34 and thus the teachings of the references fail to render the claims *prima facie* obvious. Hence, Reiter, Schweitzer, and McGauley fail to obviate the present invention as recited in claims 9, 10, 21, 22, 33, and 34. Consequently, it is respectfully urged that the rejection of claims 9, 10, 21, 22, 33, and 34 under 35 U.S.C. § 103(a) as being unpatentable over Reiter in view of Schweitzer and further in view of McGauley be withdrawn, and such a notice is respectfully requested.

Moreover, if an independent claim is non-obvious under 35 U.S.C. 103, then any claim depending therefrom is non-obvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Thus, claims 9, 10, 21, 22, 33, and 34 are non-obvious as Applicants have already demonstrated claims 1, 13, and 25 to be in condition for allowance. Applicants respectfully submit that claims 9, 10, 21, 22, 33, and 34 are also allowable, at least by virtue of their dependence on an allowable base claim.

III. <u>Conclusion</u>

It is respectfully urged that the subject application is patentable over Reiter, Schweitzer, Van Renesse, Lomet, Carey, and McGauley and is now in condition for allowance.

The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: December 06, 2004

Respectfully submitted,

Steven McDonald
Reg. No. 45,999
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Agent for Applicants

[1] The Examiner indicated in discussions conducted on November 3rd, 8th and 9th, 2004 the following correspondence between designations recited in the Office Action issued 08/06/2004 and respective passages of Reiter:
Brief Summary Text - BSTX(4) corresponds to Reiter, Column 1, Lines 19-30;
Detailed Description Text - DETX(14),(2) corresponds to Reiter, Column 6, Lines 1-12 and Lines 57-59;
Claim Text - CLTX(36) corresponds to Reiter, Column 17, Lines 23-27.

[2] The Examiner indicated in discussions conducted on November 3rd, 8th and 9th, 2004 the following correspondence between designations recited in the Office Action issued 08/06/2004 and respective passages of Schweitzer:
Detailed Description Text - DETX(71) corresponds to Schweitzer, Column 9, Lines 23-46.

[3] The Examiner indicated in discussions conducted on November 3rd, 8th and 9th, 2004 the following correspondence between designations recited in the Office Action issued 08/06/2004 and respective passages of Van Renesse:
Detailed Description Text - DETX (28),(29) corresponds to Van Renesse, Column 7, Lines 39-54.

[4] The Examiner indicated in discussions conducted on November 3rd, 8th and 9th, 2004 the following correspondence between designations recited in the Office Action issued 08/06/2004 and respective passages of Lomet:
Detailed Description Text - DETX(3) corresponds to Lomet, Column 3, Lines 10-20.

[5] The Examiner indicated in discussions conducted on November 3rd, 8th and 9th, 2004 the following correspondence between designations recited in the Office Action issued 08/06/2004 and respective passages of Carey:
Brief Summary Text - BSTX(4) corresponds to Carey, Column 1, Lines 22-32

[6] The Examiner indicated in discussions conducted on November 3rd, 8th and 9th, 2004 the following correspondence between designations recited in the Office Action issued 08/06/2004 and respective passages of McGauley:
Detailed Description Text - DETX(132) corresponds to McGauley, Column 14, Lines 56-61.